BLOCKCHAIN- KYC FOR CREDIT ALLOCATION

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING

Use Case Report

submitted by

K.SAI LALITH

22501A0584

Under the guidance of

Mr. A. Prashant, Asst. Prof.

Department of Computer Science and Engineering

Prasad V Potluri Siddhartha Institute of Technology

(Permanently affiliated to JNTU-Kakinada, Approved by AICTE)

(An NBA & NAAC accredited and ISO 9001:2015 certified institute)

Kanuru, Vijayawada-520 007

2024-25

Prasad V Potluri Siddhartha Institute of Technology

(Permanently affiliated to JNTU-Kakinada, Approved by AICTE)

(An NBA & NAAC accredited and ISO 9001:2015 certified institute)

Kanuru, Vijayawada-520 007

CERTIFICATE

This is to certify that the Use Case report entitled **"Blockchain-KYC for Credits Allocation"** that is being submitted by **K.SAI LALITH (22501A0584)** as part of Assignment-1 and Assignment-2 for the **Blockchain Technology(20CS4601C)** course in **3-2** during the academic year **2024-25**.

Course Coordinator
Mr. A. Prashant
Assistant Professor,
Department of CSE,
PVPSIT, Vijayawada

Head of the Department
Dr. A. Jayalakshmi,
Professor and Head,
Department of CSE,
PVPSIT, Vijayawada

MARKS	
ASSIGNMENT-1:	**____/5**
ASSIGNMENT-2:	**____/5**

INDEX

S. No.	Chapter	Page No.
1	Introduction	1
2	Background	2-5
3	Blockchain Basics	6
4	Use Case Overview	7
5	Implementation	8-14
6	Benefits	15-16
7	Challenges	17-18
8	Conclusion	19
9	SDG’s Addressed	20
10	References	21
11	Appendix	22

1. Introduction

Know Your Customer (KYC) is a critical process in the financial sector that ensures banks and financial institutions verify customers, establish risks, and prevent financial crimes such as fraud and money laundering. Traditional ways of KYC involve manual verifications or reliance on centralized credit bureaus, resulting in inefficiencies, rising operational costs, security vulnerabilities, and delayed processing of information. These have been a cause of concern regarding data privacy, regulatory compliance, and the performance of financial risk management. Blockchain technology offers a decentralized and secure method for KYC procedures as it allows financial institutions to access and authenticate customer information in real time without having to depend on a central entity. The fundamental aspects of blockchain such as immutability, transparency, security, and decentralization make blockchain an appropriate answer to revolutionize KYC verification. Unlike the conventional practices, a blockchain-based KYC system provides a shared, tamper-proof register ensuring customer data captured once cannot be modified and is shared exclusively with registered parties. A blockchain-based KYC system facilitates financial institutions' secure exchange of customer financial details, data integrity, regulatory compliance, and replication of real-time data. Through smart contracts, the system confirms processes in automatic mode, reducing human involvement to a lesser degree, lowering chances of error, and speeding up faster, streamlined identity confirmation. Blockchain also eliminates the likelihood of redundant verification procedures, supporting free interbank coordination while keeping customer sensitive data secured. This research explores the use of a blockchain-based KYC system in banking, focusing on its technology, advantages, disadvantages, and real-world applications. The study utilizes Ethereum smart contracts, private blockchain, and Proof of Stake (PoS) consensus algorithm for secure, scalable, and effective KYC verification. Besides, the article highlights the contribution blockchain makes toward reinforcing financial transparency, reducing the risks of fraudulent activities, and decreased reliance on third-party organizations. The decentralized framework offers immediate and accurate access to customer credit risk, limits, and collateral details, with improved decision-making and operational efficacy. The research also aims to find practical strategies towards the integration of blockchain-based KYC with well-established banking infrastructures, transcending the adoption hurdles and future directions in financial security.

2. BACKGROUND

2.1. BLOCKCHAIN TYPES

The initial process of creating a blockchain application involves choosing the right infrastructure. Four major types of blockchain networks exist, each with different features and applications. For financial institutions such as banks, the Private Blockchain Network or Consortium Blockchain Network is usually the preferred option because it provides controlled access and additional security measures. Figure 1.0 illustrates the differences between these blockchain types, showing their control mechanisms, security levels, and ideal use cases.

1) PUBLIC BLOCKCHAIN NETWORK

A public blockchain is decentralized to the point where no entity has control over the network. Everyone, or sometimes called stakeholders, has an equal right to take part in validating and producing new data blocks. The best example of such a network is Bitcoin, in which transactions are validated through consensus mechanisms like Proof of Work (PoW). Public blockchains are transparent, but they can be unsuitable for financial institutions because of scalability and regulatory issues.[1],[6]

2) PRIVATE BLOCKCHAIN NETWORK

A private blockchain is a permissioned network in which one entity can manage access and transaction validation. In contrast to public blockchains, private blockchains limit participant rights according to pre-established rules defined by the governing body. Private blockchains are often utilized for enterprise applications, government organizations, and institutions demanding additional security and efficiency. This method provides quicker processing of transactions and better privacy but could restrict decentralization.

3) HYBRID BLOCKCHAIN NETWORK

A hybrid blockchain combines aspects of both public and private blockchains. Although network access can be restricted to one entity, transaction verification can be decentralized like that of a public blockchain to guarantee more transparency and security. An example of this kind of network is the IBM Food Trust initiative that improves supply chain traceability with data confidentiality reserved for certain participants.[7]

4) CONSORTIUM BLOCKCHAIN NETWORK

A consortium blockchain is distinct from private and public blockchains in that it's controlled by a pre-selected group of organizations rather than a single organization. This system improves security with distributed verification and still has controlled access to the network. One such example is a notary blockchain network, where only notary members with

permission can be involved in governance and verification. Consortium blockchains are especially beneficial in financial services, where several banks and financial institutions cooperate while maintaining data security and compliance.

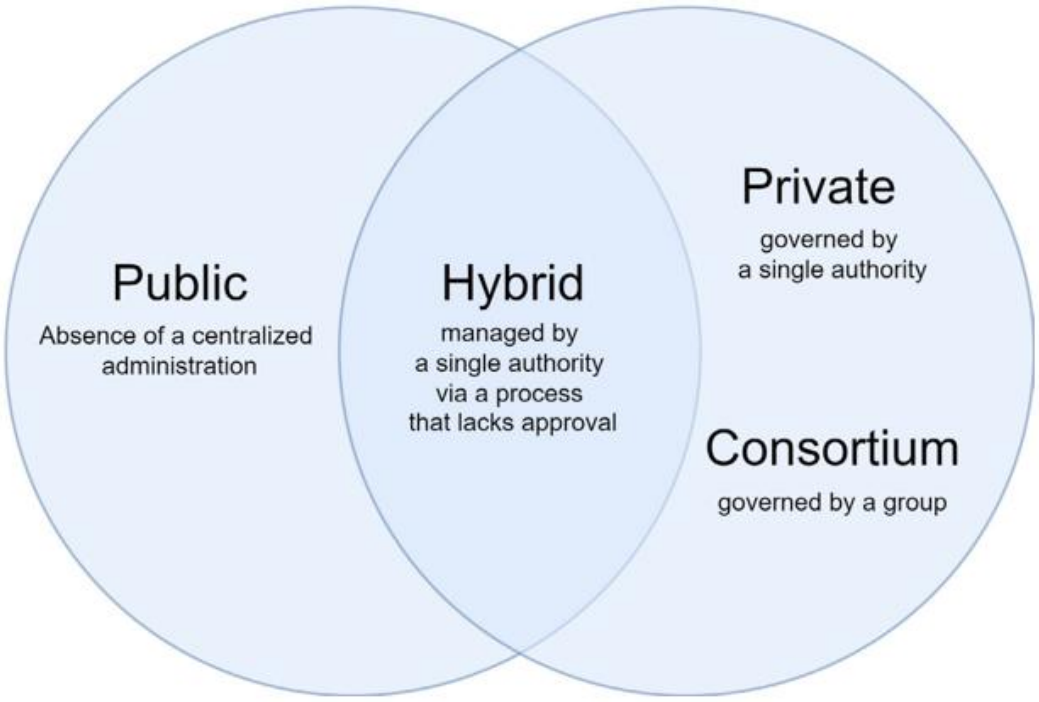

Figure2.1.0: Types of blockchain.

2.2. SMART CONTRACT

The term smart contracts coined by Nick Szabo in 1994 is used to describe self-executing computer programs deployed on a blockchain network. The contracts enforce agreements automatically when specific conditions are fulfilled, and there is no need for intermediaries. Since blockchain is immutable, smart contracts are highly secure and tamper-proof. By adopting peer-to-peer replication and decentralized execution, smart contracts provide transparency and reliability for transactions.

As investment in decentralized ledger technologies, especially blockchain, has increased, Ethereum smart contracts have picked up momentum in the financial industry. Banks and financial institutions are enthusiastically investigating their applications to simplify financial transactions, automate payments, and improve compliance with regulatory requirements. A smart contract is a code piece deployed on a blockchain that runs automatically based on pre-programmed logic, maintaining efficiency and minimizing operational risks. On the Ethereum Network, smart contracts are written in Solidity and reside immutably on the blockchain,

enabling smooth interaction between several parties. Deployed, these contracts enable secure, transparent, and tamper-proof financial transactions, making them a vital instrument in contemporary bank applications.

2.3 KYC TYPES

KYC processes entail customer identification and risk-based measures followed by financial institutions. Banks conduct such procedures for them to be aware of extensive knowledge of client profiles, trading habits, as well as expected threats related to money laundering as well as funding for terrorism. With a well-structured KYC framework in place, it becomes possible for institutions to align their service provision with customer requirements and legislatory requirements as well. Blockchain technology offers a revolutionary solution to KYC through the provision of an integrated platform for safe data storage and sharing. Unlike traditional KYC models, where customer information is stored separately in isolated banking systems, a blockchain-based KYC model provides financial institutions with a secure, decentralized means of sharing authenticated customer data. Table 2.0 summarizes the benefits of using blockchain for KYC data storage, emphasizing improvements in security, efficiency, and cost savings.[3]

SCENARIO	**DEFINITION**
Streamlined Customer Onboarding	Blockchain technology largely eliminates the necessity of re-verifying customers already on the network, thus promoting quicker onboard
Enhanced Cost Efficiency	Shared KYC services facilitated by blockchain can lead to a substantial decrease in client verification costs for participating institutions
Mitigated Fraud Risk	The immutable nature of blockchain transactions ensures the integrity of customer data, thereby reducing the risk of fraudulent information
Consent-based Information Sharing	With customer consent, only relevant KYC information is shared with new institutions, facilitating a more streamlined enrolment process
Immutable Audit Trail	All updates to customer data are permanently recorded on the blockchain, enabling easy identification of the source of any inaccuracies
Increased Operational Security	The anonymized nature of transactions on a blockchain network enhances the overall reliability and security of operations
Identify Empowerment	Blockchain technology can empower individuals, particularly refugees facing challenges in obtaining traditional documentation, by providing a secure and verifiable record of their identity

Table 2.3.1: Benefits of creating an integrated platform for safe storage of KYC data.

The traditional KYC framework employed by banks functions in silo mode, with individual banks collecting, verifying, and storing customer information independently. Blockchain-

based KYC offers a collaborative solution, where data can be accessed in real-time, duplication minimized, and fraud detection improved. Banks can help avoid the harassment of customers, who otherwise have to get verified time and again by different establishments, if they use blockchain. Figure 2 shows how the conventional KYC process differs from a blockchain-supported KYC system, highlighting how decentralized validation facilitates efficiency, security, and trust across financial ecosystems.

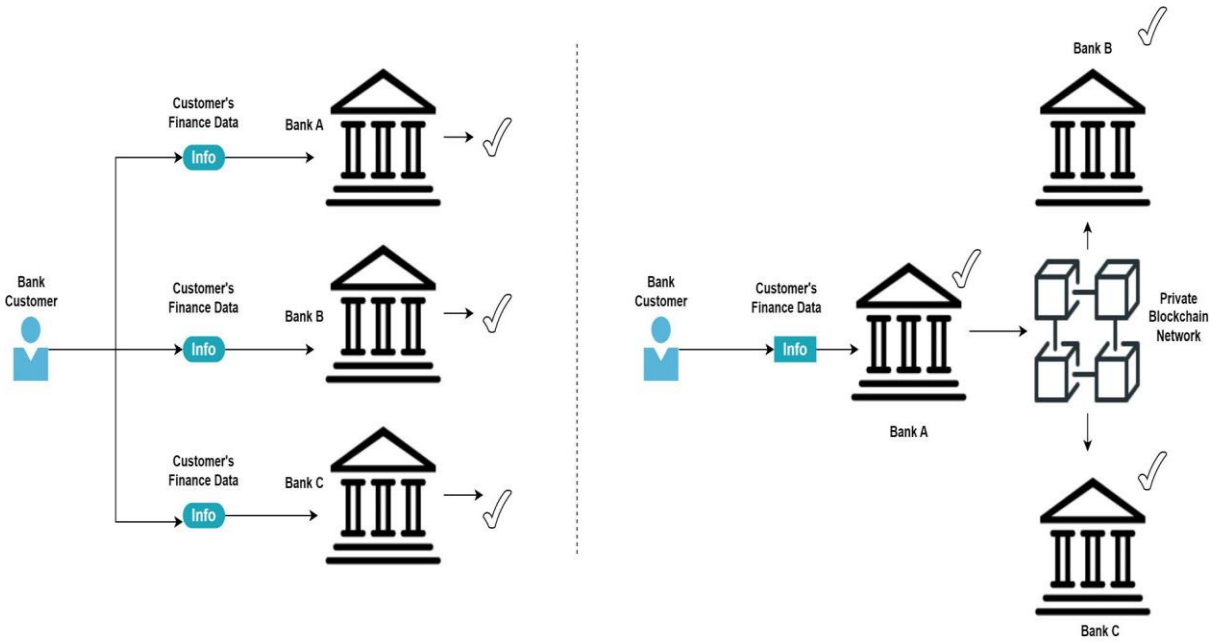

Figure 2.3.0: Traditional and blockchain based KYC Model.

3.Blockchain Basics

Blockchain revolutionizes KYC-based credit allocation by introducing security, transparency, decentralization, and efficiency into the verification and lending processes. Traditionally, financial institutions require customers to undergo KYC verification multiple times, leading to redundancy, high costs, and delays [3][7]. With blockchain, KYC data is stored in an immutable, decentralized ledger, ensuring that once verified, customer identity information can be securely accessed by authorized institutions without repeated verification. This avoids redundant work, lowers the cost of compliance, and improves the relationship of trust between financial institutions. Smart contracts are important in the automated credit dispensing by ensuring that the loan is dispensed only to customers who have met predetermined conditions.

These contracts carry out transactions without intermediaries, lowering the time for processing and eliminating human errors. Further, blockchain facilitates self-sovereign identity management where users are in complete control of their personal data, allowing access only to trusted institutions when needed. This not only enhances data privacy but also avoids unauthorized access and identity theft. Additionally, blockchain improves fraud protection and security through the guarantee that all KYC records are tamper-evident and auditable in real-time. This discourages fraudsters from falsifying information to engage in financial fraud or acquire credit illegally. Blockchain's transparency guarantees that regulators and financial institutions can simply confirm compliance, lessening the risk of money laundering and financial crime. Interoperability between various financial institutions is another benefit, with blockchain providing a single, centralized KYC database that the banks, lenders, and credit bureaus can access[6][9]. This provides a speed boost in loan approvals as credit history and KYC information are immediately verifiable. Blockchain also facilitates easier cross-border credit allocation, allowing easy lending between nations while adhering to global rules.

While its advantages, blockchain-based KYC credit allocation has its drawbacks, including scalability, regulatory risks, and cross-blockchain network interoperability. These constraints are, however, being addressed by continuous improvements in layer-2 scaling solutions, regulatory regimes, and hybrid blockchain models[1][2]. With more financial institutions embracing blockchain for KYC and credit allocation, the technology will fuel quicker, more secure, and cheaper lending processes ultimately leading to more accessible and inclusive financial services globally.

4.Use Case Overview: Blockchain-Based KYC Model

1.Traditional KYC

In traditional banking, the KYC process is highly repetitive and inefficient, requiring financial institutions to individually obtain and verify customer data. This results in redundant processes, delays in approvals, and security risks due to centralized data storage. In contrast, a blockchain-based KYC system eliminates duplicate verifications, allowing customer records to be accessed securely in real time. Table 4.2.0 compares traditional KYC models with blockchain-based KYC models, highlighting the efficiency and security improvements.

2. Blockchain-Based KYC as a Solution

A KYC model that is powered by blockchain tackles the above problems with a decentralized, secure, and tamper-evident storage and sharing system for customer data. Rather than every bank making individual KYC checks, there is a shared blockchain platform to access customer verified records in real-time. It avoids unnecessary repeat verifications and ensures quick onboarding, reduces costs, and improves security.[3],[4],[10]

Feature	**Traditional KYC**	**Blockchain-based KYC**
Centralization	Centralized	Decentralized
Transparency	Enables real-time data sharing.	Enables real-time multi data sharing.
Security	Data can be manipulated bank personnel.	The immutability of blockchain allows for tamper-proof data.
Risk Assessment	Risk is calculated only with the bank's own data.	Extensive risk assessment is made with data from other banks.
Efficiency	Repetitive verification processes among banks.	Elimination of duplicate processes.
Regulation	Governments allow centralized system.	Bank regulation needs improvement.

Table 4.0: Evaluation criteria of traditional and blockchain-based KYC

5.Implementation

A. Smart Contract Vulnerabilities in Blockchain-Based KYC

The other major issue in blockchain-based KYC systems is the exploitation of smart contract vulnerabilities. Smart contracts, or self-executing codes on a blockchain, execute KYC procedures, verify user identities, and enable interbank data sharing. But vulnerabilities in contract logic or poor security measures can result in unauthorized access or manipulation of data.

To counter this risk, financial institutions utilize stringent testing practices, security audits, and best coding practices in Solidity to ensure that smart contracts are still resilient against cyber attacks. Furthermore, using secure coding standards, periodic contract updates, and decentralized governance mechanisms also enhances the resilience of blockchain-based KYC implementations.

One of the key issues of smart contract security is the risk of re-entrancy attacks, in which an attacker may make repeated withdrawals or modify stored values before the contract can update its internal state. Another possible issue is integer overflow and underflow, which may cause the contract to behave differently than intended. Preventive measures like formal verification, secure development frameworks, and multi-signature authorization are instrumental in avoiding such risks.

The consensus mechanism, as embodied by the function:

Consensus(data)= f (blockchain nodes)

Guarantees that only authenticated participants may make contributions to the decision-making process, upholding the security and integrity of KYC records on the blockchain. Through the combination of private blockchain networks, strong consensus protocols, and high-level cybersecurity practices, financial institutions can effectively mitigate the risks posed by Sybil attacks and smart contract vulnerabilities, providing a secure, transparent, and efficient KYC verification system.

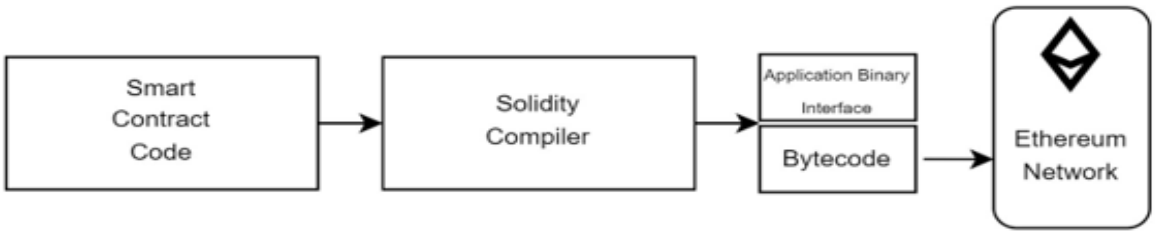

Figure5.1.0: Deployment of Smart Contract to Blockchain Network.

In front-end development, the address of the smart contract and its ABI code are important aspects. Using these features, the front-end application creates a link to the Ethereum wallet of the user using the selected provider. Importantly, sending data (e.g., logging financial data) to the blockchain has a gas cost, while reading from the existing data is generally

free. In the Ethereum blockchain, for example, the fee of a transaction is set by the cost of a computational unit (gas price) and the user-specified maximum amount of allocated computational units (gas limit), as in (1).

EQUATION5.1.0:

$$\textbf{TransactionCost} = \textbf{GasPrice} \times \textbf{GasLimit}$$

A key advantage of blockchain-based KYC is its ability to provide seamless cross-bank access to verified customer data, reducing the need for redundant verifications. This enhances customer experience, accelerates credit approvals, and reduces identity fraud risks. Figure 4 shows how blockchain enables real-time reading and writing of customer data in a decentralized network, ensuring both security and efficiency

In blockchain and distributed systems, Sybil attacks are a major concern. Sybil attacks take advantage of the system's dependence on identities by allowing an attacker to create a large number of fake identities (Sybil identities). This manipulation allows the attacker to gain excessive control over the network, which could compromise fundamental functions like consensus protocols, resource allocation protocols, and security protocols.[2],[6],[8],[10]

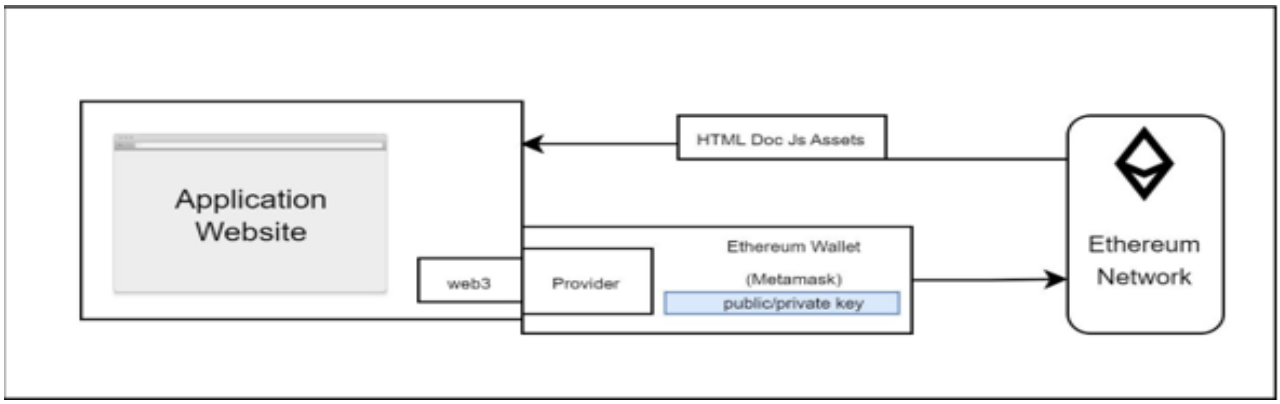

Figure 5.1.1: Reading/writing of customer's data in blockchain network.

B. Sybil Attacks in Blockchain-Based KYC

Blockchain technology offers a very secure and decentralized environment for KYC verification within the financial industry. Blockchain offers controlled data sharing along with the assurance that information stored remains tamper-proof and immutable. Yet, in addition to its security features, blockchain-based KYC frameworks are not completely secure from cyberattacks. One of the most significant vulnerabilities is the exposure to Sybil attacks when an attacker generates many fake identities to attack the network.

To mitigate Sybil attacks, different blockchain networks utilize decentralized and Sybil-resistant consensus protocols. These protocols use different validation methods, for example, voting, endorsement, and identity confirmation, to define a reliable and decentralized source of legitimacy. This approach resolves the core query of "who verifies the verifier?" by preventing the total domination of the verification process by one entity.

Through the use of multi-layered authentication and cryptographic validation, blockchain-based KYC systems seek to minimize the risk of identity fraud while ensuring system integrity.

Public blockchain networks are naturally susceptible to Sybil attacks because of their open-access nature, where any user can join without being verified. In contrast, private blockchain networks, which work within closed-down ecosystems, minimize the likelihood of such attacks since they impose controlled access and identity verification protocols. Consensus algorithms like Proof of Work (PoW) and Proof of Stake (PoS) serve to prevent Sybil attacks through the imposition on participants to put in computing resources or assets into stake, and hence discourage spoofing identity formation. In this research, it is shown how using a private blockchain framework bolstered with an effective PoS consensus protocol is capable of stemming unauthorized proliferation of identities.[2],[8],[10]

5.2 Process

1. Start

- The process starts when a customer makes a credit application.
- This step is about completing forms and providing required KYC (Know Your Customer) documents to be verified.

2. Credit Application

- The credit application of the customer is put up for review.
- This entails checking identity, financial background, and qualification criteria.

3.Eligibility Check

- The automated check is conducted by the system: "Is the Customer eligible for credit?
- This decision-making step ascertains whether the applicant satisfies the conditions needed for credit grant.
- Decision factors may be:
- Credit Score (history of repayments)
- Income level
- Existing financial obligations
- Verification through blockchain-based KYC records

4. If the Customer is Eligible (Yes Path)

- If the customer meets the credit criteria, the process moves forward to credit allocation.

Credit Allocation

- The authorized customer is credited with the desired amount of credit.
- The credit is processed and accounted for future transactions.

Transmitting Customer's Information to Blockchain Network

- The transaction and customer's KYC information are stored securely on the blockchain.
- Blockchain guarantees:

- Tamper-proof record
- Security and transparency

- Less fraud risk

Conclusion

- The process completes successfully, and the customer is granted the reserved credit.

5. If the Customer is Not Eligible (No Path)

- In case the applicant does not qualify for credit, the process stops at once.
- The customer is notified of the denial, and no credit is granted.

Important Takeaways from Blockchain-Based KYC in Credit Processing

-Security & Privacy: Blockchain guarantees that KYC information is safe and tamper-proof.

- Efficiency: Credit approval automation with blockchain accelerates the process.

-Fraud Prevention: Blockchain implementation decreases the possibility of identity theft and fake applications.

- Transparency: All approvals and transactions are registered in an irreversible ledger.

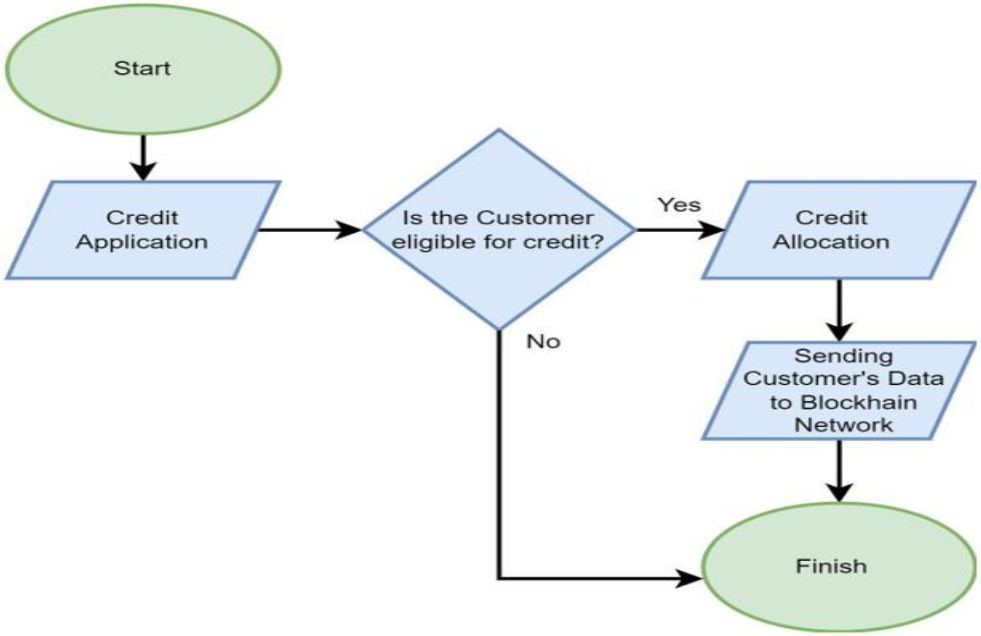

Figure 5.2.1: Process of customer credit with blockchain based KYC.

5.3 Algorithm for Blockchain-Based KYC for Credit Allocation

1. Deploy the smart contract to the Ethereum blockchain, making the deployer the owner of the contract.
2. The user gets registered by providing their name, ID proof, and credit score, keeping in mind that they are not already registered.
3. The contract saves the user's data and sets their KYC as verified.
4. The owner of the contract grants a bank by including its address in the list of authorized banks.
5. An authorized bank makes an application for credit on behalf of a user, verifying if:
5a)- The user is KYC verified.
5b) The credit score of the user is more than 700.
6. If both the conditions are satisfied, the requested credit amount is allocated to the user.
7. Authorized banks can fetch a user's information, such as name, credit score, KYC status, and approved credit amount.

5.4 Code Implementation

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract BlockchainKYC {
    struct User {
        string name;
        string id;
        uint256 score;
        bool verified;
        uint256 credit;
    }

    mapping(address => User) public users;
    mapping(address => bool) public banks;
    address public owner;

    modifier onlyOwner() {
        require(msg.sender == owner, "Not authorized");
        _;
    }

    modifier onlyBank() {
        require(banks[msg.sender] == true, "Bank not authorized");
```

```
        _;
    }

    constructor() {
        owner = msg.sender;
    }

    function regUser(string memory _name, string memory _id, uint256 _score) public {
        require(!users[msg.sender].verified, "User exists");
        users[msg.sender] = User(_name, _id, _score, true, 0);
    }

    function authBank(address _bank) public onlyOwner {
        banks[_bank] = true;
    }

    function revokeBank(address _bank) public onlyOwner {
        banks[_bank] = false;
    }

    function applyCredit(address _user, uint256 _amt) public onlyBank {
        require(users[_user].verified, "KYC not verified");
        require(users[_user].score >= 700, "Low score");
        users[_user].credit = _amt;
    }

    function getUser(address _user) public view onlyBank returns (string memory, uint256,
bool, uint256) {
        User memory user = users[_user];
        return (user.name, user.score, user.verified, user.credit);
    }
}
```

5.5 Example Scenario

Step 1: Deploy Contract
- The owner of the contract deploys the Blockchain KYC contract.

Step 2: Register a User
- Alice invokes register User("Rama", "ID1234", 750).
- Alice's KYC is labeled as verified in the contract.

Step 3: Authorize a Bank
- The owner of the contract invokes authorize Bank(bank Address).
- The bank is now authorized to act on credit applications.

Step 4: Apply for Credit
- The authorized bank invokes apply For Credit(Alice Address, 5000).
- As Alice's credit score is 750 (>700), she is granted a $5000 credit.

Step 5: Retrieve User Details
- The bank invokes get User Details(Alice Address), and it returns:
- Name: "Rama"
- Credit Score: 750
- KYC Verified: True
- Approved Credit: 5000

6.Benefits

1.Faster Processing

- Manual checks and paperwork are required for multiple traditional KYC processes, causing delays.
- Blockchain utilizes smart contracts to automate identity checks, taking a great deal of processing time off the table.[7]

2.Improved Security

- Customer data is encrypted by blockchain, which is tamper-proof and protected against cyberattacks.
- Unauthorized use is blocked by cryptographic methods and distributed ledger technology.[7]

3.Reduced Costs

- KYC verification on a manual basis consumes significant financial and human resources.
- Blockchain-based automated KYC verification lowers financial institutions' operational costs.[5]

4.Data Privacy & Control

- Customers maintain ownership of their personal information with self-sovereign identity management.
- They can provide and withdraw access to financial institutions as required for compliance with data privacy laws.[3]

5.Transparency

- Each transaction and process of identifying customers take place on an irrevocable ledger.
- This enhances banks', regulators', and customers' trust through guaranteed accountability.

6.Cross-Bank Access

- Blockchain enables financial institutions to securely share verified customer information.
- This removes duplicate KYC verification when customers seek services from several banks.[10]

7.Fraud Prevention

- By removing centralized points of storage, blockchain minimizes the risk of data breaches.
- It stops the generation of false or duplicate identities through decentralized identity verification.[3]

8. Enhanced Customer Experience

- Speedier approvals result in improved customer service.
- Avoids constant resubmission of documents.[9]

9.Global Access to Credit

- Customers are able to obtain credit across geographies without going through repetitive KYC.
- Identity verification based on blockchain facilitates financial inclusion.[9],[10]

10.Auditability and Compliance

- Regulators can ensure compliance in real-time without the need for manual audits.
- Reduces regulatory breaches and fine risks.[5],[10]

7.Challenges

1.Regulatory Compliance

- Blockchain functions in different regions, so financial institutions need to comply with different local, national, and international regulations (e.g., GDPR, AML laws).
- Some nations have stringent data privacy legislation that is incompatible with blockchain's immutability.[4],[9]

2.Integration with Legacy Systems

- Legacy banking infrastructure was not designed to handle blockchain technology.
- Integrating blockchain-based KYC with current systems demands deep software changes, expert skills, and investment.[7],[9]

3.Scalability Issues

- Public blockchains become slow and costly with increasing transactions added to them.
- Financial institutions processing millions of KYC verifications per day can be challenged with transaction speed and fees on blockchain networks.[1],[8]

4.Smart Contract Vulnerabilities

- Smart contracts are used for automation in KYC-based blockchain.
- Maliciously coded smart contracts can be manipulated by hackers, resulting in financial and data losses.[2]

5.High Initial Implementation Costs

- Implementing blockchain solutions involves investing in infrastructure, security controls, and employee training.
- Though cost saving is achieved over the long term, initial expenditures may prove challenging for small- and medium-sized financial institutions.[2],[7]

6.User Adoption and Trust

- Multiple banks, clients, and authorities lack knowledge regarding blockchain technology.
- In the absence of widespread know-how and belief, adoption would be slow and thus reduce the potential of blockchain-based KYC.[4],[9]

7.Data Immutability Issues

- Once customers' data have been entered in the blockchain, they cannot be modified or destroyed.
- This is problematic if erroneous or obsolete data must be corrected, so compliance with legislation such as GDPR's "right to be forgotten" becomes difficult.

8.Energy Consumption

- Certain blockchain networks, particularly Proof-of-Work (PoW) systems, use high levels of electricity.
- This can render blockchain-based KYC solutions less environmentally friendly.[1],[8]

9.Potential for Data Breaches in Permissioned Blockchains

- Private (permissioned) blockchains are governed by a limited number of institutions, so they still have central points of weakness.
- If the institutions operating the blockchain are hacked, user information may still be vulnerable.[6]

10.Legal and Ethical Issues

- Ambiguity over data ownership: Who owns customer data on the blockchain?
- Disputes under law can occur if customers, banks, or regulators disagree on data rights, security, or liability in case of fraud.[6]

8.Conclusion

This research has demonstrated how blockchain can transform the KYC process by providing a decentralized, secure, and efficient system for identity verification. Through smart contracts, cryptographic validation, and decentralized data storage, blockchain offers enhanced fraud prevention, seamless compliance automation, and reduced verification costs. Figure 5 illustrates how customer credit verification is streamlined using blockchain-based KYC, ensuring efficient credit approvals and financial inclusion

In so doing, blockchain technology eliminates the deficiencies of the traditional KYC in banking by using a decentralized, immutable ledger, which allows for improved customer onboarding, secures data in terms of security, and enables real-time risk assessment. Regulatory challenges do exist regardless, but blockchain brings more efficiency, cooperation, and handling of risks under a secure, open structure. As blockchain technology advances and legal frameworks develop, it can re-engineer KYC to set a new standard for secure and effective customer authentication in banking. With the speed of cross-border data growth, the need for secure storage and easy sharing between the stakeholders has become increasingly determinant. Blockchain technology is an excellent solution in this regard, making transparent and secure data exchanges possible.

This purpose is likely to be applied more broadly in the financial industry in the future. Compliance and regulatory problems persist, however. These issues will open up multiple applications in financial institutions, including the potential use of non-fungible tokens (NFTs) in the same purpose. The combination of blockchain with artificial intelligence (AI) could also further optimize identity verification operations. Banks are able to leverage AI-driven analytics on blockchain-based data to better determine risk. Smart contracts can also automate compliance verification, lowering operational expenses and human error. Lastly, improved data immutability guarantees that personal customer information is not tampered with or accessed without permission.

9.SDG ADDRESSED

SDG-9: Industry, Innovation, Technology, and Infrastructure

Justification: The Blockchain-enabled KYC framework facilitates SDG-9 through an increase in innovation, security, and efficiency of financial systems. Conventional KYC procedures are susceptible to inefficiencies, fraud, and information breaches. Blockchain offers a decentralized, immutable, and transparent system, ensuring data integrity and minimizing fraud exposure. Interbank data sharing precludes redundant verifications, simplifying financial services. Utilizing the Proof-of-Stake (PoS) consensus mechanism renders it more energy efficient compared to traditional systems. Smart contracts ensure compliance automatically, reducing cost and minimizing human intervention. Blockchain also trust and financial inclusion, particularly for underserved communities. As technology continues to advance, combining blockchain with AI and big data can further enhance fraud detection and risk assessment, enabling financial infrastructures to be more resilient and future-proof.[4],[5],[8]

SDG-11: Sustainable Cities and Communities

Justification: KYC through blockchain helps achieve SDG-11 by improving security, financial access, and urban resilience.Most people are hindered from accessing financial services because of ineffective identity verification. Blockchain provides secure, tamper-proof digital identities, which increase the accessibility of financial and government services. It decreases identity fraud and establishes trust between citizens and institutions. The energy-efficient PoS mechanism also decreases the carbon footprint of banking operations. In disaster-affected regions, immutable digital identities ensure citizens continue to have access to critical services. Moreover, integration of blockchain with smart city infrastructure enhances secure transactions, data privacy, and fraud prevention to further sustainable and inclusive urban development.[4],[5]

10.Refernces

1. S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf.
2. Ethereum Foundation, *Ethereum Whitepaper: A Next-Generation Smart Contract and Decentralized Application Platform*, 2023. [Online]. Available: https://ethereum.org/whitepaper/.
3. World Economic Forum, *Blockchain for Digital Identity: The Decentralized Future of Verification*, 2025. [Online]. Available: https://www.weforum.org/.
4. International Monetary Fund (IMF, *The Role of Blockchain in Financial Inclusion and Banking Security*, 2025. [Online]. Available: https://www.imf.org/.
5. United Nations, *Sustainable Development Goals (SDGs): Transforming Our World*, 2015. [Online]. Available: https://sdgs.un.org/goals.
6. Cointelegraph, *Blockchain for KYC: How Distributed Ledgers Are Transforming Identity Verification*, 2023. [Online]. Available: https://cointelegraph.com/.
7. S. Perera, S. Nanayakkara, M. N. N. Rodrigo, S. Senaratne and R. Weinand, "Blockchain technology: Is it hype or real in the construction industry", *J. Ind. Inf. Integr vol:17,* ppno.1-20, JAN2025 Available: https://www.sciencedirect.com/science/article/abs/pii/S2452414X20300017?via%3Dihub
8. M. Platt and P. McBurney, "Sybil in the haystack: A comprehensive review of blockchain consensus mechanisms in search of strong Sybil attack resistance", *Algorithms*, vol. 16, no. 1, pp. 34, Jan. 2025. Available: https://www.mdpi.com/1999-4893/16/1/34
9. V. D. Kolychev and D. V. Solovov, "Methods and mechanisms of a subsystem formation of financial monitoring of suspicious operations in commercial bank", *KnE Social Sci.*, vol. 3, no. 2, pp. 279, Feb. 2025, Available: https://kneopen.com/Kne-Social/article/view/1555/
10. H. Byström, "Blockchains real-time accounting and the future of credit risk modeling", *Ledger*, vol. 4, pp. 40-47, Feb 2025, Available: https://ledger.pitt.edu/ojs/ledger/article/view/100

11.APPENDIX:

The following QR code redirects to a drive folder that contains the documentation, abstract and a Video presentation of this use case
Or use
(https://drive.google.com/drive/folders/1Pl4QHWgDnhUnQe4hD5wgret0JW291Psm)